EUROPEAN PARLIAMENT

DIRECTORATE-GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT C
CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS

Constitutional Affairs

Justice, Freedom and Security

Gender Equality

Legal and Parliamentary Affairs

Petitions

Developing Biometrics in the EU

STUDY

EN FR

2010

DIRECTORATE GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT C: CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS

CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS

Developing Biometrics in the EU

STUDY

Abstract

Accepting a broad definition of biometrics to include behaviour and emotion opens the door to, and is the pre-condition, of a surveillance state of commodified citizens. Biometrics per se are not problematic: their naïve use for diverse purposes is and raises serious ethical issues about their impact on society. Naive use of biometrics compromises claimed security objectives, inadvertently imperils citizens' rights, and does not necessarily boost either interoperability at the technical level, nor politico-security goals at member state and EU level.

The paper addresses biometrics, body scanner and related issues of identity management function and mission creep. It makes suggestions for the European Parliament and national parliaments to better evaluate legislative options in order to address and safeguard citizens' liberties, privacy and data protection, avert de-sensitisation and overcome weaknesses in current legislative responses and data practices. Well-thought out ethical use of ubiquitous ICT is imperative.

PE 425.613 EN

This document was requested by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs

AUTHORS

Professor Juliet LODGE
ICT ETHICS (f7P), Jean Monnet European Centre of Excellence, University of Leeds (UK)

With Max SNIJDER (Responsible for the annexed section on Dutch passports)
JMECE and Eurobiometrics Forum

Under the coordination of the Justice and Home Affairs Section of the Centre for European Policy Studies (CEPS)

RESPONSIBLE ADMINISTRATOR

Alessandro DAVOLI
Policy Department C: Citizens' Rights and Constitutional Affairs
European Parliament
B-1047 Brussels
E-mail: alessandro.davoli@europarl.europa.eu

LINGUISTIC VERSIONS

Original: EN
Translation: FR

ABOUT THE EDITOR

To contact the Policy Department or to subscribe to its monthly newsletter please write to:
poldep-citizens@europarl.europa.eu

Manuscript completed in March 2010

This document is available on the Internet at:
http://www.europarl.europa.eu/studies

DISCLAIMER

CONTENTS

LIST OF ABBREVIATIONS

AFSJ	Area of Freedom, Security and Justice
EHRC	Equalities and Human Rights Commission (UK)
EP	European Parliament
FRR	Facial Recognition Reliability
ICT	Information and Communication Tecnology
IDM	Identity Management
IOP	Inter-operability

EXECUTIVE SUMMARY

Background

The paper addresses socio-political and ethical issues concerning the inherent naivety around the solutions and purposes of using biometrics for disparate purposes, and makes a number of suggestions and recommendations to allow the European Parliament and national parliaments to better evaluate legislative options in order to address and safeguard citizens' liberties and to find ways of overcoming the inherent weaknesses in current legislative responses.

Aim

The paper aims to show that accepting a broad definition of biometrics to include behaviour and emotion opens the door to, and is the pre-condition, of a surveillance state. It argues that sloppy data procedures de-sensitise governments, industry and the public to ubiquitous, privatised surveillance and risks commodifying and insecuritising citizens and society. It discusses body scanner and related issues, the example of the Dutch passport, and the way in which biometric use is used to facilitate functionalities creep and mission creep in policy and practice that are insufficiently controlled or controllable by public authorities. Ubiquitous ICTs make governments, businesses and citizens more vulnerable than they realise to intrusion on their privacy, their data, and their 'identity'. The risks of not remedying deficiencies lie in compounding public disaffection and distrust in political authority and facilitating a privatised surveillance state with all that implies for a loss of public accountability, openness and transparency, and greater insecuritisation of citizens. This opens the door to irrational forces opposed to the common good.

GENERAL INFORMATION

KEY FINDINGS

- The intertwining of internal (AFSJ and internal market, including sustainable economy, environment and knowledge society) policies with external security presents significant challenges to innovative thinking. Disjointed policymaking insecuritises commodified citizens and states.

- Concern over the indiscriminate and growing use of biometrics for increasingly mundane and imprecise purposes results in a breach of the earlier intention to ensure their proportionate deployment for verifying and authenticating a person's claim to a specific, context-dependent identity.

- Technological innovation, and the way in which the EU member governments have accepted a definition of biometrics originating in the discourse of the USA and homeland security agenda, has led to an unthinking culture of biometricisation and commodification of citizens and implicit acceptance of surveillance based on a loose definition of 'biometrics'. This embraces multi-model biometrics, 'second generation' biometrics (behaviour, such as key-strokes, signature and voice recognition) and 'third generation' biometrics (behaviour derived from emotion).

- Data base synergy is essential and ECHR and CFR must be respected and strengthened.

- Biometrics for the sake of biometrics disregards reliability issues and wider EU goals beyond those associated with territorial integrated border management

- Applications and policies using biometrics should be subject to stringent data protection risk assessment criteria.

- Biometricisation of citizens erodes the principle of citizen equality. It allows third states and outside interests to fragment EU privacy and protection, and exploits variable practice among the EU27 to the detriment of the EU and citizens.

- Biometricisation and digital life go beyond the pan-opticon: biometric surveillance is everywhere in some member states, and much rarer and less intensive in others. Biometrics should not be separated from egovernance and ICT use for social and commercial use in the public or private, or joint public-private sector arrangements.

- The potential for biometrics to augment security needs to be re-visited, and an effective EU privacy and personal data protection regime urgently defined and enforced across governance and commerce. No exceptions should be allowed for any aspect of outsourcing. Third parties must no longer be allowed to determine the agenda or content of rules and regulations.

- Clear distinctions must be made between using biometrics as a token to try and boost the level of trust given to the automatic 'decisions' made by machines reading biometric documents at points of entry or exit to or from territorial borders, and

their use for enabling access to goods, services, ecommerce and e-public services whether within a locality or across borders.

- The biometric is but ONE element of identification tokens used across e-transaction spaces. As such, it is tied up with interoperability, interchangeability of tokens, compatible systems, the roll-out of all e-services and e-commerce in the private and public sectors, and in public-private partnerships and in all aspects of transactions that are out-sourced.

- Biometrics is big business. Commerce in biometrically verified and verifiable identities attracts commerce and crooks. Cyber crime is growing.

- Interoperability goals to boost the competitiveness of the knowledge society must cease to be separated from the discourse over securitising territorial borders.

- The implications for citizens' and society's security from cybercrime and trade in e-identities needs urgent attention, legislation and preferably uniform definition of what constitutes a 'crime' and common penalties based on EU standards if pervasive insecurity is not to result from e-identity (mis)use.

- The overall risk is unintentional insecuritisation owing to the lag between ICT innovation and up-to-date regulatory frameworks compounded by lack of overaching common EU rules on data storage, sharing, slicing etc for diverse purposes that third parties can exploit to the potential detriment of citizens' privacy and the integrity of a data subject.

- This paper confirms the criticisms in the previous briefing paper Trends in Biometrics (2006) by Juliet Lodge [IP/C/LIBE/FWC/2005-08/SC3 PE 378.262]

1. BIOMETRICS IN PERSPECTIVE

1.1. Context: how biometrics for security problematise e-life

Biometrics for security are inextricably linked to inseparable internal and external security goals and procedures for sharing and exchanging information automatically. Biometrics per se are not a problem. How they are used is. The function and mission creep potential for using associated centralised biometric data bases provokes concern over intrusion on privacy and data protection. Generally, citizens do not have choice in opting in or out of providing biometrics. Biometrics are associated with surveillance not simply for legitimate reasons related to information exchange for improving integrated border management (eg Eurosur and Frontex)[1], but also with disproportionate, imprecise and invisible use.

Technological innovation, and EU member governments' acceptance of a definition of biometrics originating in the USA and homeland security agenda, has led to implicit acceptance of surveillance based on a loose definition of 'biometrics'.[2] The EU's recent commitment to intelligence led internal security rests on this broad interpretation of 'biometrics', and moreover on automated systems and their capacity to trigger action.

It is disingenuous to separate consideration of biometrics from any ICT process involving the transaction of any information that can be linked to an individual. Biometrics are designed to enable that. Artificial distinctions in purpose specification between electronic identity tokens (eIDs) for internal market or AFSJ – illustrated by e-services, eIDs and ejudicial cooperation - lead to unintended insecuritisation of citizens and society.

In the UK, opposition to identity cards has been ignored by softening the young public up to 'identity cards for entitlements' (such as entry to bars), and by the passport service developing an ID card function within it. Some governments, moreover, use biometrics (and EU requirements for them in travel documents) as an excuse to create centralised data bases. How biometrics facilitates this is shown in the annex on the Dutch passport.

At EU level the introduction of biometric identity documents (not an EU responsibility) have been semi-legitimised by soft law measures such as European Council conclusions. Their implementation is not subject to sufficient control or scrutiny by national parliaments or by the European Parliament. It is not acceptable to abdicate responsibility to private or semi-private-public partnerships when government and parliament should require for their measured legitimate use. Data protection bodies and ombudsmen are essential but insufficiently influential at the stage before draft rules are finalised. It is too easy for governments and commerce to proceed in defiance of them.

Biometricised e-IDs take many forms and rest on diverse and sometimes incompatible security architectures. EU member states differ over whether an e-ID should be compulsory or not, who is responsible for securing it, and over what precise form it should take. In the case of e-passports, differences remain regarding the technical specifications and standards, reliability requirements and technologies, processing, handling in respect of lost or stolen passports and visas, enrolling biometrics, and therefore implicitly over the extent

[1] Stockholm Programme p.18

[2] US VISIT *Smart Border Alliance RFID Feasibility Study*, Final Report,www.dhs.gov/xlibrary/assets/foia/US-VISIT_RFIDattachB.pdf.

to which an individual holding the passport of a given member state may be regarded as an EU citizen. The biometric eID is widely seen as something that minimises risk and boosts certainty and hence 'security'.

e-IDs are used for tracking cross border entry and exit, automated gate recognition as passengers leave airport lounges to board planes, and tracking persons and goods. They are also used for logging onto to smart phones and computers, verifying and authenticating a person's identity as they seek access to information, such as in law enforcement or health care environments. Their use in smart environments to boost the competitiveness of the EU's knowledge and information society is regularly applauded by governments. Unauthorised traceability attacks, however, facilitate tracking of an 'innocent' e-passport holder and so invade his privacy.

Controversially but increasingly, biometric eIDs are used for recording the presence of children in school (in place of verbal and written registers), and for paying for commodities and services in schools (such as drinks or lunches). They can be developed by anyone and used for any purpose. R&D to advance the e-health agenda is welcomed as an example of beneficial public-private cooperation, improved service delivery, effective and efficient governance and convenience and security gains to citizens. Problems, including insider and outsider fraud and theft, are downplayed. Disproportionate data is typically held on eID biometric cards used to prove age as a condition of legal entitlement to purchase alcohol, for example in the UK[3]. Varying data retention practices exist. Sites for data handling expand, e.g. biometrics for visas and passports (fingerprints and photographs in the UK can be enrolled at designated Home Office bureaux or at 17 registered Post Offices on payment of an extra fee); checks are out-sourced, even privatised, to agencies outside the EU. The Stockholm programme envisages a new agency developing entry exit alongside existing registered traveller programmes by 2015, a European Schengen visa, and common visa centres.

Public distrust in governments is increasingly matched by distrust in ICTs, their cost, leakiness, improper access to, and manipulation of, personal data (as highlighted by the British Home Secretary in March 2010 regarding the UK eBorders' UK Identity and Passport Service) and personal e-data. Citizens were not reassured when he confirmed that the National Identity Register held National Insurance numbers and answers to 'shared secrets'.

Biometric tools were originally intended to boost security and minimise risk for legitimate, operational security reasons. In an ambient, 'smart' intelligent, interoperable world, they potentially inadvertently add to risk and insecurity.

1.2. Maximising biometrics for EU Information Exchange and Internal Security

The *Internal Security Strategy* affirms 'anticipation and prevention' through cross-agency cooperation involving not just policing and judicial authorities and civil emergency response and planning but also domestic services, including health and welfare and an integrated, comprehensive model of information exchange based on the principle of availability. 'Intelligence sharing' 'in time to prevent crime and bring offenders to justice[4] 'advocates increasing 'substantially the current levels of information exchange…by strengthen(ing) the mechanisms which build mutual trust between the authorities responsible for ensuring

[3] Shops can be prosecuted for selling alcohol to people under 18. To avoid this, some demand the presentation of a passport before the alcohol is sold. Others required the presentation of an identity card, or the Government's identity card.

[4] http://register.consilium.europa.eu/pdf/en/10/st05/st05842-re02.en10.pdf.
Council of the EU to: Delegations Subject: Draft Internal Security Strategy for the European Union: "Towards a European Security Model", 5842/2/10 REV 2 JAI 90, 23 Feb 2010.

internal security in the EU, in order to enhance existing mechanisms, and use the Information Management Strategy to develop a secure and structured European Information Exchange Model.

'This model will include all the different EU databases relevant for ensuring security in the EU so that there can be interaction between them, as far as it is needed and permitted, for the purpose of providing effective information exchange across the whole of the EU and maximising the opportunities presented by biometric and other technologies for improving our citizens' security within a clear framework that also protects their privacy. This information exchange model must always fully respect the right to privacy and protection of personal data. If a higher level of security means an increase in data exchange, it is important that that increase be managed carefully, that it be proportionate and that it respect data protection laws' (p.13)

Is this a pious hope when so many measures implicitly imply the retention and processing of 'biometrics' in a raft of bilateral agreements as well as in Eurodac, SIS II, VIS, Prum, US_VISIT programme and the SWFIT bulk data sharing with the US, for instance[5]. While the European Parliament has had some success in blocking the latter (as of March 2010), bilateral arrangements undermine attempts to achieve EU coherence. ***This is unacceptable and insecuritises citizens***. Identity theft alone rose 20% in 2009.[6]

1.3. Risky biometrics or risky deployment?

A possibly false sense of security in a biometric identity is inferred from the claim that biometrics provide the most reliable authenticating link between a person and a claimed identity (a concept that is contingent, context dependent and varies over time), and combat fraudulent multiple IDs. The notion of the infallibility of a biometric is risky, oversimplistic and compromises individual and collective security primarily because a biometric is used as a tool for realising other purposes. Simplistic claims jeopardise legitimate use for the primary purpose.[7]

The idea of introducing stringent safeguards in the use and retention of biometrics is a response to concerns raised by citizens' groups, NGOs, the Marper Case,[8] data protection supervisors, and ombudsmen over the potential for 'harm' to outweigh 'benefits' from the increasing use of biometrics across an ever wider range of disparate policy areas.

The indiscriminate deployment of biometrics aggravates anxiety as to their disproportionate use, mission creep, the associated potential intrusiveness and potential infringements of citizens' privacy and rules on data protection, and possibilities for redress. Their discriminatory potential is misused by public and private sector applications in ways that compromise the creation and protection of a European civic identity based on common values and the Charter of Fundamental Rights.[9] Possibilities for judicial redress are compromised by cross border information exchange arrangements within the EU and bilateral accords with

[5] DG Internal Policies of the Union, Citizens'Rights and Constitutional Affairs, *Data Protection in the Area of Freedom, Security and Justice: A system still to be fully developed?* PE 410.692, March 2009.

[6] Report from financial data sharer Experian http://www.karoo.co.uk/ NewsArticle. aspx?ID= B70604161268 918583A00&category=UK

[7] See Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Programme, OJ L8 13 January 2010, p.9

[8] European Court of Human Rights –EctHR, *Case of S. and Marper versus the United Kingdom* Application nos.30562/04, Strasbourg, 4 December 2008.

[9] Communication from the Commission, Compliance with the Charter of Fundamental Rights in Commission legislative Proposals, 27.04.2005. COM(2005) 172 final

third states (such as the US)[10] not subject to EP approval, and with private bodies whose pratices, values, norms and concepts of criminal offences deviate from those within individual EU member states, and exploit intra-EU differences for bilateral gain.

Biometrics are big business[11] and integral to identity management across increasing spheres of life. The biometrics industry expects strong growth in demand over the coming year despite public sector cuts owing to the recession.

1.4. Regulating biometrics and regulating inseparable internal and external security and the associated public and private sector actors

The issues facing the regulator and parliaments derive from purpose limitation, data minimisation and purpose specification breaches in the use of biometrics sometimes embedded in systems for other purposes. Fines for data breaches may have a deterrent effect but are insufficient.Vigilance is needed regarding the implications of biometrics for compliance with data protection and privacy regulations and law, and the kind of regulatory measures needed in view of the vulnerability of identity management systems (IDM) to degradation, malevolent intrusion and cyber-attacks inter alia. These in turn raise in the minds of citizens growing concerns about (i) the potentially greater insecurity biometric IDMs imply for the citizen and his means of proving his identity, and (ii) government demands that access to public services depend on the enrolment of biometric data in identity documents used for identity management purposes that may, or may not, relate specifically to border controls and 'security' but be infinitely linkable and used for imprecise purposes.

The rationale behind ***stringent safeguards in the use*** of biometric IDMs has so far been primarily located within the discourse of their potential intrusiveness on the physical body of the individual, and on the potential that the ICT tools have for compromising privacy and data protection. Privacy protective and enhancing technologies should be mandatory.

While legal regulation has been strengthened, and the role of national parliaments and the European Parliament under the AFSJ significantly boosted, good practices and auditing, as well as improved technical specifications and programmes are vital. Compliance is often sub-optimal.

- The European Parliament should carefully scrutinise COSI and hold it accountable for action under the European Information Exchange Model and associated measures linked to enhancing border control capacity (also in third states).

The pace of technological advance still outstrips the ability of parliaments to legislate and introduce measures to safeguard citizens, deter malpractice and e-crime. Data protection authorities' concerns are insufficiently influential at drafting stage.

1.5. Too little too late? ICT innovation outstripping naive legislators?

There is contradiction and tension in what some EU governments seek (more automated exchange of information under the Stockholm Programme, often for legitimate operational purposes) and what regulators, parliaments and the European Parliament want. The latter's legitimate demands for proper consultation, transparency and accountability remains fraught, and a battle ground which tests parliamentary capacity for effective scrutiny and vigilance of the executives, and also of technological innovation. Once an issue is voiced by parliament,

[10] Council of the EU, Presidency to Delegations, *Reports by the High Level Contact Group (HLGG) on information sharing and privacy and personal data protection*, JAI 822, DATAPROTECT 74,USA102, 15851/09, 23 Nov 2009

[11] http://www.spiegel.de/international/business/0,1518,682790,00.html

it is often too late to repair or overturn government approval for actions parliaments wish to question or rule-out. This is especially likely to be the case regarding matters of 'security'.

The AFSJ is no longer the responsibility only of the EU's and member states' public authorities. As long ago as 2001, the Spanish Presidency pushed the idea and in 2007, then FSJ Commissioner Frattini noted the co-responsibility, too, of the private security sector[12]. This is about more than freedom to establish services and goods and competition policy[13], and the EP must redress and develop its role to control their operation, and any formal status for such run-for-profit bodies. That is legitimately criticised by civil liberties' groups and legal bodies[14].

Governments and their private agents are notoriously lax in respecting privacy and security in the handling of personal data, as the innumerable high profile data losses and breaches especially but certainly not only in the UK, Germany, and the Netherlands show.

- Interoperability (such as linking ehealth systems with prescribing systems, social welfare and fiscal systems) is pushed by the EU27 governments, EU Commission[15] and industry alike. Potential technical, procedural, legal, managerial and security weaknesses in realising interoperability compromise citizen privacy, individual and collective security.
- Specious claims are made by governments and industry to justify prioritising interoperability over data protection, privacy and individual security.

While governments increasingly demand and embrace biometric identity management systems (naively arguing that these will modernise, boost efficiency and effective service delivery within and across state borders), they have not yet sufficiently understood:

(i) their relevance for robust e-security, complete with understanding the need to treat e-identity management systems as part of a state's critical infrastructures requiring appropriate contingency and crisis response plans;

(ii) the possibility that citizens' trust in governments and parliaments will weaken and decline the more they are seen to be lax in terms of their own data handling arrangements (including sloppy management, data processing, data selling for commercial gain, outsourcing, preventable data losses as well as theft, mash-up advocacy, forensic readiness plans, differential data retention policies and associated funding, data archiving and retrieval systems, incompatible complex infrastructures, maintenance and updating, use of financially unstable companies)

(iii) the possibility that citizens' trust will fall in the authorities ostensibly responsible for upholding high standards of data protection and privacy codes, and those responsible for 'representing the voter' (from data protection offices and ombudsmen, auditors and regulators to regional, national parliaments and courts, and the European Parliament, and consumer protection ministers and officials) as

[12] "Security by design", Homeland Security Europe, speech by Commissioner Frattini to the EU Security Research Conference , Berlin, 26 March 2007: http://www.homelandsecurityeu.com/currentissue/article.asp?art=271247&issue=219

[13] http://ec.europa.eu/internal_market/smn/smn21/s21mn11.htm summarises findings in Single Market News No 21 (2000). COUNCIL OF THE EUROPEAN UNION Brussels, 13 December 2001 (20.12)(OR. es)15206/01 ENFOPOL 156 NOTE from: the future Spanish Presidencyto: Police Cooperation Working PartyNo. prev. doc.: OJ C 340, 10.11.1997, p. 1 Subject: Network of contact points of national authorities with responsibility for private security. Brussels, 29 January 2002 (OR. es) 5135/02 ENFOPOL 5 LEGISLATIVE ACTS AND OTHER INSTRUMENTS Subject : Initiative of the Kingdom of Spain on the setting up of a Network of contact points of national authorities responsible for private security http://www.statewatch.org/news/2002/apr/priv07245.pdf
As under 29 April 2004 Case C-171/02: Commission of the European Communities v Portuguese Republic based on *Articles 39 EC, 43 EC and 49 EC — Directive 92/51/EEC*

[14] http://www.statewatch.org/news/2002/apr/priv15206.pdf

[15] http://ec.europa.eu/information_society/activities/health/index_en.htm

governments side-step or ignore their advice and/or compromise their opportunities to insist on robust regulation appropriate to EU requirements

(iv) the possibility that citizens' trust in law enforcement and policing authorities will fall and be compromised as (a) cross-border automated information exchange and cross-border mutual access to information by 'foreign' agencies grows; and (b) civil-criminal law distinctions become fuzzy and therefore open to private security agency involvement

(v) the possibility that citizens' belief in the trustworthiness of governments authorities claims to uphold law and justice will be compromised by their apparent failure to prevent 'corrupt' agencies accessing information, harvesting data, using web analytics (such as Phorm), stealing personal data and personal identity documents

(vi) the possibility that the assumed bonds of trust and accountability between citizens and governments and parliaments will be severely challenged and tested

(vii) the possibility of greater confusion if clarity is not achieved regarding ediscovery (among the EU27 and vis-a-vis the USA and other third states[16]), data archiving and retrieval and the mix of public-private agencies in the broad field of security and the application of 'security' technologies to domestic policies and fields

(viii) their role as a key in operationalising proactive intelligence led approaches to security and border management

(ix) Wide definitions of 'biometrics' facilitate mission creep that compromises civil liberties.

2. DISPROPORTIONATE BIOMETRICS: A PROBLEM OF MISSION CREEP

Mission creep arises from the multifaceted, multidimensionality and inseparability of internal and external security. It is entrenched by privatising security, by vested commercial and industrial interests looking to boost their market share, by scattered outsourcing, public and private partnerships not amenable to sufficient parliamentary control, and semi-privatising and outsourcing public administration.

Mission creep is endemic in the application of biometrics, as *Trends in Biometrics* confirmed in 2005[17]. Specious, misleading, implausible, unclear and contradictory approaches abound in their advocacy and use by the public and private sectors. The argument that biometric data is not personal data is implausible because unless linked to the person, the biometric data is not that useful. That is why its primary use was initially for territorial border controls, in identifying potential suspects likely to endanger collective security.

Mission creep in deploying biometrics is matched by mission creep in policies on exchanging information across and among agencies within and beyond the EU 27, in the type and range of biometric information to be taken directly (by intrusive) technologies, or indirectly (by 'remote' or non-invasive technologies not requiring direct physical contact with the data subject, such as cctv, temperature monitoring, gait analysis).

Mission creep is often justified on the grounds of functional purpose exploitation which may be necessary to address new purposes using existing capabilities. Mission creep

[16] O.Proust & C.Burton, 'Le conflit de droits entre les regles americaines de e-discovery et le droit europeen de la protection des donnees a caractere personnel…entre le marteu et l'enclume', Revue Lamy Droit de L'Immateriel Fev 2009:79-84

[17] IP/C/LIBE/FWC/2005-08/SC3 PE 378.262

insufficiently and inadequately respects the principles of necessity and proportionality and legitimacy of processing that form the basis for the relevant Community regulatory instruments for the information society. They are linked to the principles of being the *minimum* necessary to meet specified objectives; enhance legal certainty; and be technologically neutral. These principles mean that instruments should not exceed what is necessary to achieve the objective in question.

Biometrics are a feature of communication technologies (ICTs). Their disproportionate use and the lax and arbitrary way in which they are defined and implemented endangers values, norms and practices central to accepted conceptions in the EU27 of transparency, data protection and data privacy. Concern over the indiscriminate and growing use of biometrics for increasingly mundane and imprecise purposes results in a breach of the earlier intention to ensure their proportionate deployment based on the principle of necessity. Deviation from this is now justified by reference to loose arguments about the alleged 'certainty' that biometric identifiers bring.

The problem is that reliance on 'certainty' encourages groupthink and reliance on automated decisionmaking that exacerbate risks.

3. CHANGING BIOMETRICS

3.1. From hard to soft biometrics

Biometric standards change overtime. Common standards across IDMs would assist interoperability - a general goal of governments and ICT vendors.[18] Biometric measures differ and are not equally reliable or appropriate. Technical specifications and technological legacies, obsolescence, cost, ageing and adjustments significantly affect deployment, and compromise reliability.

Earlier this decade, the European definition and understanding of 'biometrics' was based on a measurement of a given visible and *unique* physical feature of a person – such as a fingerprint, several fingerprints, a hand or palm print, voice or iris print. By contrast, the USA defined a biometric to include a person's visible characteristics (for example gait), behaviour and associations.

Now, in both the EU and elsewhere, the definition of a biometric has been stretched to include invisible characteristics of a person. This embraces behaviour and emotion, including 'liveness tests', face dynamics, psychological states, level of arousal (fear, anxiety, intent), and body cells, fluid or traces (such as DNA, and brain imaging for forensics in crime detection). The relatively high spoof potential of first generation biometrics partly accounts for interest among border security agencies in multi-modal biometrics, including anticipatory gestures, paralinguistics and thermal imaging. But the EU's requirement is for travel documents to hold two first generation biometrics by 2019.

The therapeutic uses of medical technology (such as magnetic resonance imaging, electroencephalogrammes, and scanning) have been captured as shown as a 'biometric' that can be re-applied for use in 'security' arenas.

- Fragmented adoption of different biometrics and fragmented practice = erosion of citizen equality, privacy and security, and fragmented leaky borders

3.1.1. Body scanners

Whole body imaging – bodyscanners (first developed in 1992)[19] are the most public newish technology providing a 'biometric measurement' of a person's physique. Biometric scanners can be calibrated and set to different levels of resolution for matching the biometric presented (for example finger print ; or fingerprints for multiple applications or those for highly secure applications, either alone or with cryptology) to that stored on a travel document or data base. They can be risky.[20]

Rejected by the 2004-9 European Parliament as excessively intrusive on personal privacy, criticised as such by the British Information Commissioner commenting on their roll-out at British airports, the body scanner involves gender discrimination and discriminates among EU citizens from different states because each state, for the moment, decides locally on the type of equipment used at border posts. Body scanners have been set to 'protect' male sensitivities more than female sensitivities. Religious concerns have been raised, including

[18] ISO/IEC 247 13-1
[19] X-ray security screening system (The Secure 1000) was developed in 1992 and commercialized by RAPISCAN, http://www.dspguide.com/secure.htm
[20] The Sunday Times 5 April 2009 suggested match levels were lowered to 30% to allow entry when queues at migration post became congested.

by the Pope before his impending visit to the UK.[21] He stressed the need to balance the dignity of the person and security imperatives. Fragmented adoption and fragmented practice = erosion of citizen equality, privacy and security, and fragmented leaky borders

3.2. Fragmenting citizen equality, privacy and security

3.2.1. Fragmentation in technology

How biometrics are taken (enrolled), how they are stored and what technical equipment and local practices are adopted varies within and across the EU27. A fragmented approach to testing biometric components and systems compromises quality, the predictive ability and reliability of given biometrics over time. The cost of the technology bought and local administrative practices vary greatly and undermine citizen equality. Enrolment practices differ and exacerbate problems of (un)reliability. Imperfect enrolment and mistakes are notoriously hard to correct later. If a 69% 'match' between the live finger and the stored template is considered acceptable, deterioration over time may suggest that the verification is impaired. Fingerprint tampering has commercial potential, and the use of fake or altered fingerprints by people seeking entry to states occurs. Newer or more mobile means of capturing biometrics, IDM and verifying identity include latest generation mobile phones. Technical problems remain. Mobile biometric scanners cannot (yet) be used effectively against biometric data enrolled in stationary environments.

3.2.2. Fragmentation in practice: the problem at the territorial border posts

Differential technology, practice and interpretation and implementation of local codes of practice aggravate discrimination. The EU urgently needs to adopt and enforce uniformity in line with European goals and values : delay results in the agenda being set by third states. The EU has supervisory power : how airport security is implemented remains a member state prerogative which can be influenced by outside commercial and government interests.

- *An implausible rationale is used to justify the tendency to refer to practice in the US as a legimating rationale for disproportionate and privacy invasive use of biometric 'scanners' and data.*

The EU-US joint declaration on aviation security accepted 'enhanced technologies'. In the EU and elsewhere support grows for privacy by design, privacy enhancing technologies, baked-in security and privacy to guide against disproportionality.[22] But, a security rationale undercuts what the public infers about them, compared to what technical 'filters' ICT developers produce that allow the private and public sector purchasers to continue using them. That applies to body scanners. Body scanners are not universally used at EU entry and exit points : this results in discrimination within a state and across the EU. Theoretical opt-outs from scanners and alternative security checks (like the pat down) discriminate against travellers. The UK 2010 Code of Practice[23] prohibits the selection of travellers for security checks based on gender, race etc but this does not meet the generic criticism of discriminatory intent and impact.

---

[21] Papal audience on 23 Feb 2010 to representatives of Ente Nazionale per l'Aviazione Civile Italiana (www.enac-italia.it) and Ente Nazionale per l'Assistenza al Volo (http://www.enav.it/portal/page/portal/PortaleENAV/Home) responsible for airport workers. http://212.77.1.245/news_services/bulletin/news/25164.php?index=25164&po_date=20.02.2010&lang=en

[22] Ann Cavoukian, Information and Privacy Commissioner of Ontario , "Whole Body Imaging in Airport Scanners: Activate Privacy Filters to Achieve Security and Privacy", March 2009.

[23] UK Dept. for Transport, *Interim Code of Practice for the Acceptable Use of Advanced Imaging Technology (Body Scanners) in an Aviation Security Environment,* http://www.dft.gov.uk/pgr/security/aviation/airport/

Contrary to EU policy,[24] and views from the Commission's consultation of the EDPS, Article 29 Working Party[25], and Fundamental Rights Agency on their use, travellers refusing to use the scanners at specific UK airports can be prevented from travelling.

The Commission's public-private consultation on this ducked the issue pending an EU health and safety impact assessment[26]. Division was clear in January 2010 : some wanted common rules and single Regulation on their use, others responsible for the AFSJ supported rolling out ICTs, biometric border controls and greater information exchange among a growing web of agencies.

The EU Information Society Commissioner[27] belatedly underlined growing concern about the intrusive impact of biometric border controls, like scanners. Marking Data Protection Day, she said :

In our external relations we should firmly promote fundamental rights including the right to privacy and protection of personal data. **The right to data protection should also be respected when performing simple operations like transferring money, booking a flight ticket or passing a security check at the airport** .Why should citizens have to reveal their personal information in order to prove that they have nothing to hide?

Acknowledging citizens' calls in responses to the **public consultation** on the reform of the General Data Protection Directive for stronger and more consistent data protection legislation across the EU will be meaningless unless robust and consistent legislation follows swiftly.

- *Technological advance and mission creep suggest that it is already (almost) too late.*
- Division and inconsistency in the EU27 among governments and EU institutions allow others to set the agenda.

3.2.3. Fragmenting security through inconsistent ICT enabled leaky borders

Cross border exchange of information, whether automated or not, geared to combating serious international crime and illegal movement of goods, services, capital and persons is essential in sustaining the EU's goals and area of freedom, security and justice within the common external border.

Entry and exit to and from that bordered space, however, is regulated differently and so fragments the border (owing for example to variable membership of Schengen and compliance with its requirements, Schengen 'readiness' as measured by levels of pre-existing compliance with the rule of law and reduction of corruption among law and judicial agencies).[28] Controls are fragmented and variable around the external border and 'exported' to posts outside the EU (eg in North Africa) or at the domestic border controls extended from one member states to inside other member states (such as at Eurostar

[24] TRAN/D/2008/57605, 26.09.2008. http://ec.europa.eu/transport/air/consultations/2009_02_19_body_scanners_en.htm; EP Hearings, Summary of hearing of Viviane Reding - Justice, fundamental rights and citizenship; Commission's Green Paper on detection technologies in the work of law enforcement, customs and other security authorities, COM(2006) 474 final.

[25] http://ec.europa.eu/justicehome/fsj/privacy/indexen.htm; http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2009-others_en.htm

[26] http://ec.europa.eu/transport/air/consultations/doc/2009_02_19_body_scanners_questionnaire.pdf October 2008, the first comprehensive Privacy Impact Assessment for Whole Body Imaging was published by the *US Department of Homeland Security*

[27] http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/16&format=HTML&aged=0&language=EN&guiLanguage=en

[28] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Examining the creation of a European Border Surveillance System (EUROSUR) Brussels, 13.2.2008, COM(2008) 68 final Commission Communication, on an entry/exit system at the external borders of the European Union, facilitation of border crossings for bona fide travellers, and an electronic travel authorisation system, COM(2008) 69 final, Brussels, 13.2.2008

terminals) and at sea[29]. Over 30 different agencies are already involved in border controls in the EU and data is accessed and exchanged with many others outside the EU.

The security rationale and administration-gain rationale and logic of e-cooperation and data linkage for law enforcement, border controls, judicial and police cooperation, combating internet crime, paedophile and trafficking networks have proved compelling for governments and the EU. Inconsistent practice among the member states over how and for how long, and at what cost to whom, they process, store, link, retain, outsource, mine or sell on biometric information (both in its narrowest and in its widest senses) means that the data subject's integrity and identity are open to being compromised. The German government more recently began to argue for privacy and data protection after court rulings outlawing lengthy data retention. Bilateral agreements moreover allow even greater inequality and inconsistency. Often vilified, the UK is not alone in having a relatively poor record in public sector handling of personal data.

Much of the law, responsibilities and accountability mechanisms remain unclear to or inaccessible by citizens. Regulations on citizen redress against data degradation, theft, loss, fraud by governments, public and private sectors whether inside the EU or beyond its borders may have been created with good intentions, but they remain out of the reach of the average citizen and beyond the capacity of the most vulnerable. 'The road to hell is paved with good intentions'.

Contradictory rationales abound. There is much rhetoric around forensic readiness, data handling cultures, e-disclosure and risk management approaches to data management, much is made of an intention. At the same time, other branches of government are pushing steps to boost the potential for data mash-ups (and associated income generation).

- There should be common standards on core technical aspects ***and*** on the release and ***use*** of data
- Coherence and consistency in imperative in internal and external security – gaps in EU legislation and data protection should be urgently sealed

The EU's Internal Security Strategy pays scant attention to the known (and notorious) problems of data loss and data leakage in domestic public and private systems (eg Deutsche Bahn, Telekom, the British National Health Service).

3.3. Fragmentary approaches = arbitrary security and privacy

Discrimination arises from differential and variable technological capabilities, costs and practices regarding access to, retrieval, retention and use of 'new' biometrics such as DNA samples (which can be accessed under Schengen rules and under the Prum treaty by different agencies exchanging information), or 'behavioural' biometrics.

DNA samples are taken and stored for different purposes and according to different definitions of 'offence' for different periods of time in the EU27. In the UK, the EU state with the largest DNA database and a weak record on erasing DNA samples, using mobile biometric technology, a DNA sample can be taken from anyone suspected of an 'offence', including at the roadside for a traffic infringement. In some states, DNA is kept for many years, in some until after death, in others until the data subject is a specified age or for one hundred years (and then erased to release storage capacity)[30].

[29] European Commission Communication on the creation of a European border surveillance system (EUROSUR), COM (2008) 68, 13.2.08

[30] M.J.Beloff QC in August 2009, when asked to advise the Equality and Human Rights Commission whether the [British] Government's proposals for a National DNA database set out in a consultation document from the Home Office on "Keeping the Right People on the DNA Database" comply with the European Convention on Human Rights stated that 'if the proposals were enacted into law they are likely to breach the Convention and lead to findings of

The DNA issue illustrates a generic problem of allowing inconsistency to persist. The inevitable disproportionality and discrimination associated with this is amplified and aggravated by disparate, incompatible and quickly obsolete (but expensive) ICT systems. These magnify a further discrepancy among those able to afford 'state of the art' systems and robust security architectures, and those unable to do so.

- privacy and security against intrusion should not be hijacked by capacity to pay.
- baked in security should be the norm and the precondition demanded by all parliaments at all levels before they agree to legislation incurring expenditure on ICTs or on any upgrades of existing systems or those associated with them, like for example VIS, CIS, Eurodac, Frontex, Europol, Eurojust, SIS II amd Eurosur.
- The EDPS' supervisory, consultative and coordinating responsibilities for them must be reviewed annually to make them as strong as possible
- EU institutions and agencies (including the European Council and the various formations of the Council, diplomatic service and internal security agencies) should be required to submit proposals and measures (especially for soft law) to the EDPS, Art 29 committee and European Parliament, as appropriate, *before* decisions are taken[31]; and *should be required* to explain giving 'just cause' why their views are adopted or rejected. The EDPS should have a right of reply in such instances with public debate in the European Parliament *before* the final decision is taken.
- Steps should be taken to 'repatriate' processing and storage to in-house networks and in-house clouds.
- Outsourcing to the private sector is expensive, risky and potentially counter-productive.
- ***The broad definition of 'biometrics' should not be accepted as legitimate if a surveillance state and society is to be avoided.***

Biometrics currently means anything and everything that anyone wanting to form a 'profile' of a person (whether as a would-be migrant, tourist, student, person working with vulnerable people, or suspect) wants it to mean for their own benevolent or malevolent purposes. A 'biometric' can be captured by technologies either designed specifically for surveillance or usable for 'tracking' purposes, so biometrics are inevitably associated with surveillance.

4. DISPROPORTIONATE (IN)SECURITISATION OF CITIZENS?

4.1. (Un)ethical discrimination, insecuritisation and arbitrary intent

Biometric surveillance is everywhere in some member states. It erodes citizen equality and goes beyond the informatisation or algorithmatisation of the body. The implicit purpose of 'invisible control' is facilitated by unthinking or naive adoption and commissioning of technological applications that are faulty, potentially endanger privacy and data protection and inadvertently, because used for generic rather than specific purposes, pose risks to

violations by the European Court of Human Rights. In practice, it is unclear whether much has changed as a result.'

[31] Peter Hustinx on Data retention directive.
http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PublicationsSpeeches/2009/09-05-14_Brussels_data_retention_EN.pdf

citizens' personal privacy and security. The contribution 'new biometrics' make to collective security has yet to be adequately proven. The expense of data storage, access, retrieval and inputting makes 'security' as well as privacy dependent on capacity to pay.

- Soft biometrics raise serious ethical questions about the nature of society being created. Understanding of discrimination is blinkered by a focus on racial and gender issues. The socio-political element and detrimental implications for all sectors of society – whether handicapped, ageing, socially excluded, young, ill, political dissidents or simply 'different' – can be manipulated by authorities in line with arbitrary intent. How and why biometrics are used to discriminate opens the door to pervasive insecuritisation of individuals and society at the very time that a privatisation of security is expanding and an 'all-government departments' approach to intelligence-led internal security is advanced by the EU.

There is an unthinking adoption of technologies designed for one purpose when it is obvious that they can be used for others. The principles of data minimisation, purpose limitation, proportionality, purpose minimisation are laudable but too easily disregarded by the vendors of the technologies concerned with market share and commercial gain. This is exemplified by tracking technologies used for commercial and government security or welfare purposes. These are the tip of an ice-berg at a time when smart devices, ambient intelligence environments, ubiquitous robots, and nano technologies not only enable but depend on tracking. There is insufficient protection against data misuse, mash-ups and mission creep.

4.2. Unethical Insecuritisation and commodification of citizens?

Stretching biometric applications (in the security discourse of certainty in minimising risk and insecurity) to include behaviour opens the door to illiberal scope for discrimination, further excludes the handicapped and vulnerable, creates inequality and disproportionality that either ignore, elude or pay lipservice to data protection and data privacy regulations and intentions, device controls, data loss prevention and infrastructure management. Automating profiling or verification on the basis of 'biometric' matches breaches chains of duty and trust. Risks are compounded by ICTs and how they are used notably in disproportionate, unethical and potentially illegitimate ways. Disparate practices undermine the rhetoric of biometric certainty, yet law enforcement bodies, notably in the UK, want blanket tracking. This involves an invisible 'authority'; skews choice; and commodifies citizens.

5. COMBINING BIOMETRICS FOR SECURITY: THE EXAMPLE OF THE NETHERLANDS

Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents requires 'only' the storage of biometric information in order to verify (a) if the holder genuinely belongs to the passport and (b) the authenticity of the document. But some member states are considering (and some already have implemented supporting legislation) to store the biometric data in a central registry also for reasons that go beyond the purposes outlined in (EC) No 2252/2004.

A striking example is a recently passed law in The Netherlands, which stipulates the formation of a central national biometrics registry for the purpose of duplicate checks during the application process *and* for detection and prosecution purposes. Despite several attempts by the European Parliament to clarify with the European Commission the legitimacy of this law in the perspective of Art.8 of the ECHR, the responses of the European Commission left this question unclarified. The main argument was that the installation of a national biometrics repository alongside the passport application process is

purely a matter of national legislation. **(See Annex 1).** Yet, some British lawyers suggest that it is potentially unlawful.

Major problems for accountable and legitimate regulation arise because governments contrive to evade scrutiny and control, leaving parliaments to catch-up. Amending legislation later is difficult as they know. Soft law abounds with weak controls and inadequate levels of knowledge about the respective technologies and the possibilities opened by them. National parliaments, with a strong EP, must ensure accountability and legitimacy. There is an urgent need to re-assess the scope of the framework decision on data protection for law enforcement purposes before realising the principle of availability and widespread inter-operability of 'biometric' data, and to set out an EU model on biometricised e-governance.

6. RECOMMENDATIONS

It is no longer sensible to regard a biometric as having neutral socio-economic, or legal and political impacts. Because newer generation biometrics are fluid and add to physical measurements, behavioural and emotional data that can be combined with other data, a range of issues need to be reviewed *together. They need to be reviewed in the light of the increasing privatisation of 'security' that escapes effective, democratic parliamentary and regulatory control and over-sight at national, international and EU levels.*
The intertwining of internal (AFSJ and internal market, including sustainable economy, environment and knowledge society) policies with external security presents significant challenges to innovative thinking. Disjointed policymaking insecuritises citizens and states.

Intelligence led internal security rests on a broad interpretation of 'biometrics', and on automated systems. For civil liberties and democratic values to be upheld, public accountability through parliamentary cooperation between national and the European parliaments is vital and must urgently be strengthened to ensure consistency and to insist on robust encryption and data and purpose minimisation.

It would be appropriate to set up a small EU level non-governmental study group to investigate legislative feasibility of, and the ways forward, to:-

1. Abandon the two biometric identifiers for epassports 2019 and associated costly investment in already obsolete technologies and their supply, maintenance and upkeep
2. Harmonise PNR agreements in line with EU values and norms, and reduce current divergences in practice
3. Insist that any data exchange with any third party anywhere is based on complete reciprocity
4. Harmonise rules on retention of 'biometric' 'samples' (such as DNA, and cells)
5. Review with a view to rejecting behavioural and emotional 'biometrics'
6. Minimise data disclosure by insisting on encryption and systems that cannot interrogate all the information held on a biometric token (such as an ID card)
7. Enforce purpose limitation
8. Move from setting minimal mandatory standards for data enrolment, handling and associated processes to **set high level mandatory standards**
9. Monitor system performance, compliance annually with major simultaneous public debate in EP and national parliaments
10. Introduce urgently mandatory high level (not minima) codes of practice
11. Be clear about the benefits to the citizen and society : just because industry claims a convenience gain to citizens of onetime data enrolment does not mean that duplicate identity data does not exist elsewhere about the same citizen, nor that duplicate data standards and formats in different systems compromise the efficiency gains attributed to interoperability when tehnical interoperability itself is

compromised by legacy standards and systems,as well as technical capacity and the standards for and kind(s) of biometric associated with given data.

12. Clarify informational privacy for multiple identity tokens and documents
13. Create a common EU standard in place of divergent national standards
14. Revisit the impact on AFSJ goals and wider EU goals of divergence in data retention and retrieval policies and costs on net service providers that hamper timely lawful investigation for 'security', but also potentially compromise citizen equality.
15. Legislate on the quality and accreditation of forensic and law enforcement communicators
16. Set up rules on disclosure and unlawful disclosure to and by humans and other machines by net providers in the commercial field, and those in public-private partnerships, especially disclosure without the data subject's explicit knowledge and consent by reconsidering data encryption, device controls and infrastructure requirements and management in view of pervasive ambient intelligence
17. Re-regulate redress in view of its inaccessibility and infeasibility to most citizens and set up a meaningful ethical swift redress against identity theft
18. Review chains of duty and trust in cyber space
19. Insist on foreseeable, specific, essential and clear safeguards in the use of personal data for 'security' reasons and for 'lower level' general reasons
20. Make the principle of the data subject in control of his data the norm not the exception
21. Review the relevance of the ePrivacy directive to all ICT enabled transactions
22. Hold a wide-ranging, informed public debate on the ethical issues raised by 'biometrics', which should take place at EU level and also at the levels closest to citizens
23. An ethical code on using biometrics is imperative for all aspects of life, not just 'security'
24. Biometrics working groups should include an independent member charged with reviewing the ethical impact of biometric IDs and automated information exchange for whatever purposes
25. The European Parliament should carefully scrutinise COSI and hold it accountable for action under the European Information Exchange Model and associated measures linked to enhancing border-control capacity (also in third states).
26. The European Parliament should require that a risk impact assessment for all e-activities and R&D includes high specification technical provisions to safeguard privacy
27. Urgently review and strengthen the EP's role vis-a-vis 'private security' and the Internal security strategy and its implementation

The broad definition of 'biometrics' should not be accepted as legitimate if a surveillance state and society is to be avoided, and if citizens' privacy and data are to be protected, and security in the wider sense safeguarded.

SELECTION OF REFERENCES

Commission of the European Communities (2007) Communication from the Commission to the European Parliament and the Council on *Public-Private Dialogue in Security Research and Innovation*SEC(2007) 1138; and SEC(2007)1139 COM(2007) 511 final Sept 2007

Commission of the European Communities(2009) Amended proposal for a Regulation of the European Parliament and of the Council concerning the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Reegulation (EC) No[.../...] COM(2009) 342 final, 10 Sepember 2009.

Commission of the European Communities(2004) *Proposal for a Council Regulation on standards for security features amd biometrics in EU citizens' passports* . COM(2004) 116 final. 18 Feb 2004.

Commission of the European Communities (2005) Proposal for a Council Decision concerning access for consultation of the Visa Information System (VIS) by the authorities of Member States reponsible for internal security and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences, COM(2005) 600 final, 24 Nov 2005.

Commission of the European Communities (2009) Communication from the Commission to the European Parliament and the Council *An Area of freedom, security and justice serving the citizen* COM(2009)262/4, 25 Nov 2009.

Council of the EU to: Delegations Subject: Draft Internal Security Strategy for the European Union: *Towards a European Security Model*, 5842/2/10 REV 2 JAI 90, 23 Feb 2010.cd. http://register.consilium.europa.eu/pdf/en/10/st05/st05842-re02.en10.pdf.

Council of the European Union (2009) Proposal for a Council framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, doc.5618/09, 23 January 2009.

Council Regulation (EC) No 2725/2000 concerning the establishment of Eurodac for the comparison of fingerprints for the effective application of the Dublin Convention, 15 Dec 2000.

De Brouwer, E (2009) Towards a European PNR System? Study for CEPS on behalf of the EP LIBE Committee, 2009.

European Data Protection Supervisor –EDPS (2008), Opinion of the European Data Protection Supervisor on the draft Proposal for a Council framework Decision on the use of Passenger Name Record (ONR) data for law enforcement purposes, OJ C 110/1, 1 May 2008.

EDPS(2008), Opinion of the European Data Protection Supervisor on the Final Report by the EU-US High Level Contact Group on information sharing and privacy and personal data protection, 11 November 2008.

EDPS Third Opion of the European Data Proection Supervisor on the Proposal for a Council framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ C 139/1 23 June 2007.

Europol (2007) US-Europol cooperation agreements:
http://www.europol.europa.eu/legal/agreem,ents/Agreements/16268-2.pdf
http://www.europol.europa.eu/legal/agreem,ents/Agreements/16268-1.pdf

Eurojust,US-Eurojust agreement
http://www.eurojust.europa.eu/official_documents/Agreements/061106_EJ-US_cooperation_agreement.pdf

Agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security, OJ L 204, 4 August 2007, p.16

Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Programme, OJ L8 13 January 2010, p.9

Hayes, B 'Homeland Security comes to Europe' http://www.statewatch.org/analyses/no-90-homeland-security-comes-to-europe.pdf

House of Lords European Union Committee, The *EU/US Passenger Name Record (PNR) Agreement*, 5 June 2007---The *Passenger Name Record (PNR) Framework Decision – Report with Evidence*, London 11 June 2008.

Lodge, J (2007) A Challenge for Privacy and Public Policy – Certified Identity and Uncertainties. *Regio*:193-206.

Monahan T, Wall T, (2007), Somatic Surveillance: Corporeal Control through Information Networks, Surveillance & Society, 1:154-73.

Privacy International (2009) Statement on proposed deployments of body scanners in airports, 31/12/2009,
www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-565802

Proust,O & C.Burton, 'Le conflit de droits entre les regles americaines de e-discovery et le droit europeen de la protection des donnees a caractere personnel…entre le marteu et l'enclume', Revue Lamy Droit de L'Immateriel Fev 2009:79-84

UK Dept. for Transport, *Interim Code of Practice for the Acceptable Use of Advanced Imaging Technology (Body Scanners) in an Aviation Security Environment*,
http://www.dft.gov.uk/pgr/security/aviation/airport/

7. ANNEXES

7.1 Case Study Overview: the new Dutch Passport Act

Prepared by Max Snijder

On 9 June 2009 the Dutch Senate passed the new Dutch Passport Act. This foresees embedding the EU regulation on the inclusion of biometric identifiers in the passport chip. On top of that, it facilitates the establishment of a central fingerprint database, to provide information about individuals for :

1) preventing and combating fraud involving travel documents and the abuse of said documents
2) identifying the victims of catastrophes and accidents,
3) investigating and prosecuting criminal acts, and
4) investigating actions posing a threat to the security of the State and other important interests of one or more countries of the Kingdom or the security of powers friendly to the Kingdom

Furthermore the act states that issuance of personal information under the provisions of the above mentioned purposes may be permitted to the following entities, as provided by a "General Administrative Order":

1) government entities, where the issuance of the information is essential to the carrying out of their duties;
2) institutions and persons having a justified interest, as regards the performing of a legal obligation of identification, in the issuance of information contained in the travel document registers.

A "General Administrative Order" does not require approval by Parliament or the Senate and thus can escape public debate in the parliament and senate.

In the opinion of the CBP (College Bescherming Persoonsgegevens, the Dutch Data Protection Authority), the new passport act is "a serious infringement of privacy that is not justified by the aims to be achieved by the Act". The CBP calls for the Act to be reviewed. Nevertheless, the new act has passed the Parliament and the Senate. Starting on September 21st the Dutch authorities will start with collecting the fingerprints of every passport applicant.

It is not only the CBP that has expressed its concerns. Also privacy organizations and experts have mentioned the risks for the privacy of citizens.

Earlier, at European level, a proposal for a European Central Passport Register was brought to a halt by fierce criticism from the European Parliament. In Germany the proposal for a central biometric database also was rejected. In December 2008 the British government was blown the whistle by the European Court of Human Rights on a large scale DNA and fingerprint database, similar to the proposed Dutch central fingerprint database. The Dutch government officials insist that the DNA case is of a different nature and therefore does not affect the new Dutch passport act.

It is noteworthy that the Passport Act was adopted with so little discussion. The law contains two goals which are hard to reconcile (i) to combat identity fraud and (ii) identification of suspects/criminals. CBP Opinions in 2001 and 2007 were clearly critical about this mix of functionalities and "function creep", but ultimately had no influence on political decision-making (see also part 3), or public opinion.

Although the Senate during their discussion on June 9th didn't consider it to be necessary to consult the CBP again, the International Committee for Human Rights of the UN saw

reasons to ask questions. In front of the committee, the Minister stated that “eventually” the fingerprint could probably be better replaced by an iris code (ie the colored part of the eye around the pupil). The investigating authorities could than no longer use the database. That would take away important sensitivities around the new Passport Act (source: NRC, July 16th 2009).

This raises new questions.

Is the Minister now to believe that iris scans would eliminate many sensitivities surrounding such a database? Or does the minister "eventually" want the iris print to be saved in the passport only, and not in a central database? And what does the minister exactly mean by replacing fingerprints by iris scans "eventually "? What do we do with the central storage of the fingerprints in the meanwhile?

The offical information from the Ministry of Internal Affaires towards the Dutch citizens (i.e. a printed brochure and the Q&A on www.paspoortinformatie.nl) regarding seams not to mention the full purpose of storiing the fingerprint data outside the passport chip in a central database.. The Ministry notes the following explanation:

“The purpose of the storage of fingerprint records in the travel document administration, whether centrally or decentrally, is to ensure the reliability of the application process and issuance of travel documents. (...)
Additionally, the new administration provides the option to all passport authorities to verify for each applicant, based on the facial image, fingerprints and sex, if the person already requested a travel document under a different identity.”

The purpose of investigating and prosecuting criminal acts is not mentioned.

Although the Deputy Secretary of State of the Ministry of Internal Affaires states that the central fingerprint database never being used for “fishing” (i.e. 1:n search based on fingerprint only), it is not clear how the access to the database is being regulated and secured. In the Senate she stated that extension of the use of the database will be a matter to be judged by her successors.

Conclusions CBP regarding new Dutch Passport Act

The following passages are a selection from the report prepared by the CBP dd. March 30, 2007 "Change advice about the redesign of the Passport Act in connection with the travel documents administration” (ref.: z2007-00010). The response of the Minister of Justice dated March 17, 2009, left the opinion of the CBP unaffected (Source: CBP).

1. In the CBP’s opinion, the Act does not comply with Article 8 of the ECHR because a proper analysis of the advantages and disadvantages of central travel document registers is not included. Alternatives such as a decentralized system with a central reference index are not discussed.
2. The intended central travel document registers are irreversible and will attract the interest of other persons and organizations due to the personal information stored in it. There is a risk of function creep and the Act does not exclude this.
3. Due to technical shortcomings, large-scale application of biometrics has serious consequences for a large number of citizens.
4. The infrastructural facilities needed internationally to exchange information in a responsible manner are very extensive and their implementation presents security risks. There is insufficient attention given to the question of the consequences of a ‘break-in’ of the system.
5. Objections are being expressed at home and abroad to central travel document registers containing biometric data. The risks of abuse, improper and unforeseen use have been pointed out. The notes do not include a sufficient analysis intended to eliminate these objections.

CBP:
"In view of the above, this Act is, in the opinion of the CBP, a serious infringement of privacy that is not justified by the aims to be achieved by the Act. The CBP calls for the Act to be reviewed."

The European Court for Human Rights

The Dutch law maker has decided to store the fingerprint data in a central database, as the law now describes. These data are being said to be accessable only under strict conditions. But as may be clear from the law text, these data are not only to be used for combating identity fraud with passports and making the passport issuance process more secure. The information from this database can also be used by the public prosecutor for the purpose of determining the identity of a suspect or convicted person, or in the interest of in the interests of a criminal investigation if a crime for which (temporarily) detention is authorized. That implies that in cases of criminal offences (such as theft or physical abuse) it will be possible to provide fingerprint data if that will be in the interest of a criminal investigation. However, in this case this will be possible with the data of all citizens who are in the possession of a (valid) Dutch passport, whether or not they are supsected or convicted.

During the debate in the Dutch Senate on June 9th the Deputy Secretary of State of the Ministry of Internatl affaires stated that the Marper case didn't have any relevance to the Duthc paspport act. But it is questionable if that is a correct statement. Several questions are being raised on how the Dutch Passport Act relates to the protection of civil rights and liberties of European citizens as laid down in the European Convention on Human Rights (ECHR). What dangers are lying in the central storage of biometric data of a whole population when it comes to misues and fraud?

A case in which the European Court makes a ruling on the storage of biometric data of citizens who have proven to be innocent is the case *S. and Marper vs the UK the "(Marper case")*. This case comes the closest to the situation of biometric storage of all citizens. Firstly the court rules that the storage of a person's biometric data is part a his/her private life. Furthermore the courts points out that objectively are containing unique information of a person, which makes it possible to identify this person in a variety of situations. The court's conclusion is that storing the fingerprints is consituting an interferrence in a person's private life. However, under certain circumstances such an interferrence can be justified, if only justified by good reasons by law. In the *Marper Case* the court came to the following conclusion:

'125. In conclusion, the Court finds that the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences, as applied in the case of the present applicants, fails to strike a fair balance between the competing public and private interests and that the respondent State has overstepped any acceptable margin of appreciation in this regard. Accordingly, the retention at issue constitutes a disproportionate interference with the applicants' right to respect for private life and cannot be regarded as necessary in a democratic society.
This conclusion obviates the need for the Court to consider the applicants' criticism regarding the adequacy of certain particular safeguards, such as too broad an access to the personal data concerned and insufficient protection against the misuse or abuse of such data.

126. Accordingly, there has been a violation of Article 8 of the Convention in the present case.'

It is questionable on which arguments the Secretary of State's statement is based that the Marper case is not relevant to the Dutch Passport Act. Further elaboration and review is needed.

So how is the storage of the biometric data of all Dutch citizens justified? According to the *Marper Case* the aim of detection and prosecution would not have enough justification. It is for that reason that several Dutch citizens have started a lawsuit against the Dutch government. But if it is expected that the Dutch government will give maximum resistance, it can take up to almost 10 years before the case will reach it's final stage at the level of the European Court. In the meanwhile the storage will continue and a way back will be more difficult.

Does the technology adequately support the requirements?

The first discussions and studies on deploying biometrics for combatting identity fraud (i.e. look alike fraud) date from 1999. TNO (independent research organization for applied technologies) produced a critical report on the deployment of biometric technologies for security applications on national scale, and later (2002 and 2004) by studies on public acceptance and the suitability of face recognition and fingerprint recognition for nationwide roll out. These were all based on the pre-assumption that biometric technology was meant for combating identity fraud and to secure the passport application process, i.e. to store the biometric on the passport chip only. Under political pressure the debate slowly moved towards the addition of a centralised fingerprint database and towards additional functionalities such as detection and prosecution. But in the public discussions and debates the additional functionalities have not been mentioned openly and clearly, nor in the studies concerning the technical suitability and public acceptance. Over ten years of political debate the requirements on the biometrics for the Dutch passport has been moving, resulting in unsufficient insights in the actual intention of the law which has been in the making during the same period. If the requirements are constantly changing, how could the assessment be done that the technology is fit for its purposes? How could proper measures be proposed and developed which would deal with the intrinsic flaws of any currently available biometric technology?

The importance of quality

One important example is the quality of the enrolment. If this was analysed well against the proper requirements, the processes and procedures at the front desks for applying a passport would have been designed with strict quality requirements. Especially if the biometric data are being stored centrally for the purpose of preventing identity fraud, stringent measures should be taken to ensure that:
1) the quality of the biometric images is maximized
2) the possibility of enrolling fake fingerprints is prevented at all times and
3) that the newly produced passport is issued to the right person and that the citizens can check whether his/her biometric data are stored correctly in the passport chip.

ad1) image quality
It is well known (e.g. based on European studies such as MTIT (www.mtitproject.com) and BioTesting Europe (www.biotestingeurope.eu)) that defining the quality of a given image of a fingerprint or face is not trivial. Although there is an ISO standard on image quality, there are different interpretations of those standards by the various vendors of biometric technologies. The impact of low image quality on the matching performance (both 1:1 as 1:n) is dramatic. Performances can easily drop from a FRR of 1% to 40%. It has been scientifically been proven by NPL (UK) and Fraunhofer Institute (Germany) that the differences between biometric vendors increase strongly if the quality of the images drops. That means that strong measures on image quality will always pay off and are crucial for the long term performance of the system. However, the reality of taking the biometric data from the Dutch citizens has proven to be far removed from that:

- facial images are taken from a picture, which the applicants bring with them. In the political debate they are choosing to support the professional photographers industry

(who saw a part of their business disappearing if the passport pictures would be taken by the communities themselves), rather than choosing for security. We know from border control authorities that it is difficult for a front end operator to stay alert for longer than 15 minutes when comparing the picture on the passport with the person in front of him. This is the core challenge of the look-alike problem, which the biometric passport is supposed to solve in the first place. When a life picture is being taken at the moment of application, one can be sure that the picture will match the right person. If a picture is made by a third party (and maybe has been manipulated) and being brought at the point of application, it is relative easy to bring a picture of somebody else who looks like you and enrolled it into the system. The look alike problem will then be imported into the core of the system meant to prevent just that.

- a front end operator needs to be very alert to make sure the right fingers are enrolled. If not, it will be easy to enrol with the wrong fingers, so applicants can use another finger under another name next time
- the current procedure is that from all the captures, the ones with the best quality will be stored. Also if that quality is poor, the alternative will be a failure to enrol and that is something which needs to be avoided. Procedures will take longer, citizens are going to complain. If this happens frequently, the database will get empty spots because fingerprints are missing. People can deliberately damage their fingers in order to force a bad quality enrolment or even failure to enrol.

ad 2) the possibility of enrolling fake fingerprints is prevented at all times
In the context of preventing identity fraud this is the weakest link. Untrained operating personnel will have the greatest problems in detecting fake fingerprints. These silicon layers containing the fingerprint of another person are difficult to detect. Close inspection is needed to prevent these prints being enrolled. If not, identity fraud right in the source will be established, leaving the following consequences:

- people can enrol under their own name, but with the fingerprints of another person
- people can enrol multiple times under another name, using different fingerprints every time
- people can enrol under another name, using fake fingerprints belonging to that person whose name they use. Once stored in the central database these types of identity fraud will be very hard to detect. Once a person's identity is stolen using one of these methods, it will be almost impossible for the victim to prove his/her innocence.

ad 3) issuing the newly produced passport to the right person
In order to serve the principle of combating identity fraud, the biometric passport provides the unique opportunity to make sure that the passport is being issued to right person by performing a biometric verification at the moment of issuance (applicants still have to appear in person to get the new passport handed over). Although this biometric verification of the passport holder is the first and main reason for the European regulation EC 2252/2004, the Dutch Ministry of Internal affairs gave explicit instructions not to perform such a biometric verification at issuance. It has not been explained why this verification should not take place. One can only guess; maybe there are doubts on the performance and does it need to be avoided to get false rejects and/or public figures on false rejects as that might foster doubts on the effectiveness of the biometric passports as a whole. Additionally, a biometric verification at the moment of handing over the new passport is needed in case a citizen wishes to check whether his/her biometric data are being stored correctly. According to the Dutch law a Dutch citizen has the right of checking whether the stored data are correct. That also counts for the fingerprint data. It will create a very nasty situation if a mistake of the biometric data comes out at later, e.g. when a person's passport is being checked at the border.

Reliability of the biometric database

In discussions with forensic experts of the NFI (Netherlands Forensic Institute) and of the Dutch Police it became clear that with the current biometric enrolment process (see above),

a database that will be populated by 17 million records and only four fingers to be enrolled, a reliable 1:n search is not to be expected. That implies that under the current conditions the central biometric database will not be able to serve one of its primary requirements, i.e. to prevent identity fraud. Therefore, its establishment will hardly be proportional to the investments to be made and the price the Dutch have to pay by handing over a large quantity of their privacy.

No studies so far have quantified the benefits which the central fingerprint database would give in terms of saving costs in the issuance process, reduction of identity fraud etc. There has not been informed debate on the added value of the Dutch Passport Act. Opinions of experts and authoritative organisations have not been sufficiently taken into account. In some cases they have been ignored, as the CBP concluded.

Conclusions

Given current knowledge, the following conclusions on the Dutch Passport Act can be drawn:

- ten years of political and ministerial debate on the biometric passport preceding the newly adopted Passport Act seem to be characterised by changing requirements, insufficient public debate and a lack of input from experts.
- there is a gap between the final functional requirements as laid down in the Dutch Passport Act and the studies and pilots done in the past. The change of requirements (mainly the move from storage on the chip only to additional central storage of the fingerprint data) has not led to sufficient additional studies and analysis to make sure that the implementation of the technology and the performance expected from it are based on realistic measurements.

It is likely that the current implementation of the central fingerprint database (and all the associated processes, procedures and human interactions) increase rather than decrease the risk of identity fraud and pose a potential larger negative impact on the victims of such fraud.

7.2 Question by the European Parliament to the European Commission 21-7-09 by Jeanine Hennis-Plasschaert (LIBE)

Introduction

As a result of prolonged international and European consultations (resulting in Regulation 2252/2004, and later followed by 444/2009) a facial scan and two fingerprints will be stored in the passport as from October. The aim is to avoid identity fraud.

The Netherlands has now decided on a central storage of biometric data and an associated detection function for law enforcement purposes. With this the Dutch authorities failed to take sharp criticism from home and abroad, and in fact makes every Dutch a suspect in advance. Inter alia function creep, fraud and misuse (or: abuse) are real risks. Furthermore, the recent statements of the Dutch Minister of Justice for the International Committee of the UN Human Rights ("the fingerprint should be replaced by an iris code") are striking to say the least.

Questions 1st Term

- Has the Commission been consulted on the proposal by the Netherlands to a central storage of biometric data and to an associated detection function?
- What is the Commission judgement on the new Dutch Passport Act under the proportionality principle? Please a concrete answer.
- What is the Commissions judgement on the new Dutch Passport Act regarding the individual privacy? Please a concrete answer.
- Does the Commission consider the new Dutch Passport being in accordance with Article 8 of the ECHR? If so, why? If not, why not?
- Does the Commission consider storing biometrics in the passports only will be more than sufficient for an effective fight against identity fraud? If not, why not?
- Does the Commission consider that, if already decided to storage in a database, a distributed storage (with central reference index) would suffice? If not, why not?

Questions 2nd Term

- Has the Commission been consulted on the proposal by the Netherlands to a central storage of biometric data and to an associated search and detection function for law enforcement purposes?
- does the Commission consider it likely that a central storage of biometric data associated with a search function is conditionally needed in the interest of public safety or the protection of the public policy?
- Does the Commission consider storing biometrics in the passports only will be more than sufficient for an effective fight against identity fraud? If not, why not?
- Does the Commission consider that, if already decided to storage in a database, a distributed storage (with central reference index) would suffice? If not, why not?

7.3 Article: What does the Dutch Minister of Justice Hrisch-Ballin want with the new passport act?

Source: NRC, 24 juli 2009

Last week the United Nations experessed their concerns on the new Dutch Passport Act. The response by Minister Hirsch Ballin (Justice, CDA) in Geneva is far from reassuring. Last week the International Committee for Human Rights (ICHR) of the United Nations Geneva has questioned the Dutch minister Hirsch Ballin (Justice, CDA) about the status of human rigths in The Netherlands. The potential consequences for the civil rights of the New Passport Act where on the agenda. This act will get into force on September 15th.

The recently adopted law provides for the establishment of a central database with fingerprint data of all Dutch passport holders. On top of that, public prosecutors get access to the database for law enforcement purposes under conditions. The Human Rights Committee strongly suggested some critical questions about the compatibility of the database with Article 8 of the European Convention of Human Rights (ECHR). It was to be expected that this committee was going to express it's concerns. The Dutch Data Protection Authority (CBP), biometrics experts and (international) lawyers have repeatedly stressed the undesirability of central storage of fingerprint data relating to the right to privacy and unacceptable security risks.

What has been of very great surprise were the remarks Hirsch Ballin made in Geneva. It was only in June of this year that in front of the Dutch parliament the Dutch government declared that its concerns regarding the new Passport Act where unfounded by declaring the risks as being insignificant and the privacy violation proportional. Now, just a few weeks later, the minister admitted that maybe the wrong type of biometrics was chosen.

Indeed, after the first hearing the minister said not be excluded that the fingerprints "eventually" should be replaced by the iris. With that statement the minister apparently tried to respond to criticism of the UN Committee on the detection element of the Passport Act. A database of iris scans instead of fingerprints would no longer be interesting for the detection services, was apparently the idea of the minister.

This suggestion of the minister is remarkable, partly because one of the pillars of the new Passport Act was designed to facilitate that detection element. How should we interpret this? Is this about a review of the minister of a recently approved act by the parliament? For the record: the European agreements require that the passport chip next to the already introduced biometric facial scan a second biometric feature should be included - eg the fingerprint or iris scan. With the inclusion of a fingerprint or an iris scan in the passport chip The Netherlands would indeed meets to all its European commitments.

But as said, the Dutch government goes beyond what European legislation prescribes, and additionally goes to save biometric data in a central database to combat identity fraud from September.

Is the Minister now to believe that iris scans would eliminate many sensitivities surrounding such a database? Of course, the iris, unlike the fingerprint, is not a traditional evidence in criminal proceedings. The point is that the current state of the iris technology already is capable - without the person being aware – to make photos of his iris to compare with stored iris prints. It is therefore possible that in the future an iris database creates in fact the same detection opportunities as the fingerprint database of the current act. Or does the minister "eventually" want the iris print to be saved in the passport only, and not in a central database?

Anyway, the exact intentions of the minister in Geneva are not understood. Why has the parliament stressed the importance of the detection capability and why are not alternative biometrics and considerations presented?

And what does the minister exactly mean by replacing fingerprints by iris scans "eventually "? What do we do with the central storage of the fingerprints in the meanwhile? As already mentioned, the new act will get into force on September 15. For Dutch diplomats abroad, the law is already in force since last August. We can only guess. With the mention of the iris as an alternative in the face of an authoritative UN committee the chance that the Passport Act is brought before the European Court of Human Rights has increased significantly. In December 2008 the same court blew the whistle against the British government on a large scale DNA and fingerprint database.

Meanwhile, the European Parliament also posed questions about the Dutch law to the European Commission, including whether it is not contrary to Article 8 of the ECHR. Sweden, the new EU president, has put the protection of civil rights and privacy high on the agenda. Last week the European Ministers of Justice reached agreement on this in Stockholm.

"Strong European law includes guarantees for civil liberties," said Minister Hirsch Ballin on this occasion. He added that he considers joining the EU to the ECHR a realistic ambition. If we "eventually" change to iris scans for privacy reasons, wouldn´t it be wise to hold of the creation of the central fingerprint database for the coming years?

= = =

7.4 The introduction of biometric indentifiers

Originally *five* proposals from EU institutions led to the introduction of biometric identifiers:

1. **24 September 2003**: Proposal for a Council regulation amending (EC) 1683/95 (uniform format for VISA) and (EC) 1030/02 (uniform format for residence permits)
2. **8 June 2004**: Council decision (2004/512/EC) establishing the VISA Information System (VIS)
3. **13 December 2004**: Council regulation (EC) 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States
4. **28 December 2004**: Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay-visas, COM(2004) 835 final;
5. **28 February 2005**: Commission decision C (2005) 409 laying down the technical specifications on the standards for security features and biometrics in passports and travel documents issued by Member States23.

The EU planned to use biometric systems at its various land, sea and air borders in order to monitor all non-EU nationals admitted to the Schengen zone, starting from 2015. All third country nationals who need a visa to enter EU territory are registered in the Visa Information System (VIS). Name, address, occupation as well as visa-application history, biometric photograph and fingerprints are stored and available for immigration and law enforcement purposes

EUROPEAN PARLIAMENT

DIRECTORATE-GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT C
CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS

Role

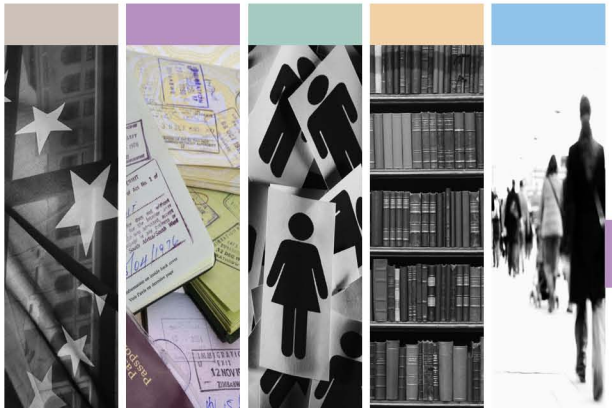
Policy departments are research units that provide specialised advice to committees, inter-parliamentary delegations and other parliamentary bodies.

Policy Areas

- Constitutional Affairs
- Justice, Freedom and Security
- Gender Equality
- Legal and Parliamentary Affairs
- Petitions

Documents

Visit the European Parliament website: **http://www.europarl.europa.eu/studies**



ISBN